



①9 BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENTAMT

⑫ **Offenlegungsschrift**
⑩ **DE 196 48 767 A 1**

⑤1 Int. Cl.⁶:
G 07 C 9/00
G 07 F 7/10
G 06 K 19/07
A 61 B 5/117

②1 Aktenzeichen: 196 48 767.6
②2 Anmeldetag: 25. 11. 96
④3 Offenlegungstag: 26. 6. 97

DE 196 48 767 A 1

BEST AVAILABLE COPY

③0 Unionspriorität: ③2 ③3 ③1
21.12.95 AT 2084/95

⑦1 Anmelder:
Siemens AG Österreich, Wien, AT

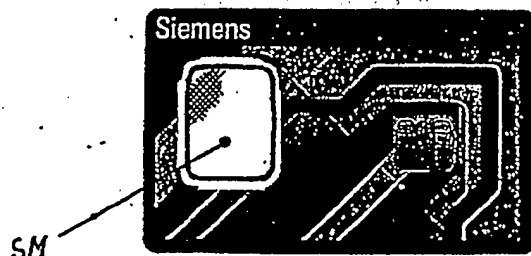
⑦4 Vertreter:
Fuchs, F., Dr.-Ing., Pat.-Anw., 81541 München

⑦2 Erfinder:
Rechberger, Rudolf, Steinriegl, AT

Prüfungsantrag gem. § 44 PatG ist gestellt

⑤4 Identifikationssystem mit elektronischer Chipkarte

⑤7 Es wird ein Identifikationssystem mit elektronischer Chipkarte, mit Speichern (VSL) für biometrische Identifikationsmerkmale der benutzungsberechtigten Personen, mit Sensoren (SM) zum Erfassen der biometrischen Identifikationsmerkmale und Mitteln (VSL) zum Vergleich der gespeicherten und der erfaßten biometrischen Identifikationsmerkmale angegeben, bei dem die Mittel zum Speichern, zur Erfassung und zum Vergleich der biometrischen Identifikationsmerkmale jeweils zumindest teilweise in der Weise in die Chipkarte integriert sind, daß ein autonomer Vergleich der gespeicherten mit den erfaßten biometrischen Identifikationsmerkmale möglich ist. Damit ist eindeutige und manipulationssichere Personentifizierung ohne PIN-Nummer oder Foto möglich.



DE 196 48 767 A 1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 04. 97 702 026/685

5/25

Die Erfindung betrifft ein Identifikationssystem mit elektronischer Chipkarte, mit Speichern für biometrische Identifikationsmerkmale der benutzungsberechtigten Personen, mit Sensoren zum Erfassen der biometrischen Identifikationsmerkmale und Mitteln zum Vergleich der gespeicherten und der erfaßten biometrischen Identifikationsmerkmale.

Die Verbreitung und Vermarktung von Dienstleistungen, bei denen auf geschützte Daten zugegriffen werden muß, erfolgt in zunehmendem Maß mittels Systemen zur elektronischen Datenverarbeitung, wobei elektronische Chipkarten eine wesentliche Rolle spielen. So werden sie beispielsweise bei den sogenannten Geldausgabautomaten in Verbindung mit einer individuellen Kennung — der PIN-Nummer — zur Berechtigungsüberprüfung verwendet, oder auch als elektronische Geldbörse, auf die Geldbeträge aufgebucht werden können, die dann im bargeldlosen Zahlungsverkehr in Geschäften durch entsprechende Chipkarten-Schreib/Lesegeräte wieder abgebucht werden.

Durch die Kombination von Chipkarte und PIN-Nummer wird zwar die Wahrscheinlichkeit einer mißbräuchlichen Verwendung verringert, gleichzeitig aber auch der Komfort für den Benutzer verringert, die Fehlerhäufigkeit bei den Bedienvorgängen erhöht und der Vorgang der Berechtigungskontrolle verlängert, was beispielsweise in Hauptgeschäftszeiten zu erheblichen Wartezeiten und Warteschlangen vor den Geldausgabautomaten führt.

Erschwerend wirkt sich dabei auch der vielfältige Einsatz verschiedener Chipkarten für die unterschiedlichsten Services in der Telekommunikation, bei der Zutrittskontrolle zu Hochsicherheitsbereichen wie Rechenzentren, oder im Gesundheitswesen aus, so daß sich der Anwender für den Einsatz der verschiedenen Chipkarten auch unterschiedliche PIN-Nummern merken muß.

Viele Benutzer notieren sich daher die PIN-Nummer und verringern damit die Sicherheit der Kombination Chipkarte-PIN-Nummer ganz beträchtlich.

Insbesondere für Zutrittskontrollen werden daher bereits Systeme angeboten, bei denen auf einer Chipkarte biometrische Daten — beispielsweise ein Fingerabdruck — eines Berechtigten gespeichert werden, die im Anwendungsfall, bei der Zutrittskontrolle von einem Kontrollgerät, meist einem Personalcomputer mit einem angeschlossenen Sensor mit dem Fingerabdruck des Benutzers verglichen werden, und bei Übereinstimmung der beiden Abdruckdaten der Zutritt freigegeben wird.

Aus der WO 94/25938 ist weiterhin ein System zur Fingerprint-Identifikation bekannt, bei dem ein Fingerprint-Sensor in eine Chipkarte integriert ist.

Nachteilig an den genannten Systemen ist insbesondere, daß sicherheitsrelevante Daten — die Information über den Fingerabdruck — von der Chipkarte auf ein Kontrollsystem übertragen werden und damit ausgespäht werden können.

Der Erfindung liegt daher die Aufgabe zugrunde, ein Identifikationssystem anzugeben, das höchsten Sicherheitsanforderungen genügt.

Erfindungsgemäß geschieht dies mit einem Identifikationssystem der eingangs genannten Art, bei dem die Mittel zum Speichern (VSL), zur Erfassung (SM) und zum Vergleich (VSL) der biometrischen Identifikationsmerkmale jeweils zumindest teilweise in der Weise in

die Chipkarte integriert sind, bei dem ein autonomer Vergleich der gespeicherten mit den erfaßten biometrischen Identifikationsmerkmale möglich ist und kein Austausch sicherheitsrelevanter Daten zwischen der elektronischen Chipkarte und den übrigen Komponenten des Identifikationssystems erfolgt.

Für die Identifikation geeignete personenbezogene Merkmale sind beispielsweise das Muster der Blutbahnen der Netzhaut, die Struktur der Iris, die Länge und Form der Finger, das Gesicht, die Stimme oder aber Fingerabdrücke. Die Möglichkeiten, Personen aufgrund dieser Merkmale zu identifizieren, sind beispielsweise in IEEE Spectrum, Februar 1994, "It had to be you" beschrieben. Die wahrscheinlich am besten erforschten und damit zuverlässigsten Merkmale sind dabei die Fingerabdrücke, wobei durch Überprüfung mehrerer Fingerabdrücke noch die Zuverlässigkeit erhöht werden kann. Diese sind auch in für den Benutzer komfortabler Weise zu ermitteln, während z. B. das Muster der Netzhaut nur durch eine für den zu Identifizierenden unangenehme Prozedur erfaßt werden kann und daher nur in jenen Fällen angewendet werden wird, in denen dieser Effekt keine Rolle spielt oder ggf. sogar erwünscht ist.

Vorteilhaft ist es, wenn die Sensoren zum Erfassen des zumindest einen Fingerabdruckes ein Transistorarray beinhalten, und wenn die Transistoren so geschaltet sind, daß das thermische Abbild des zumindest einen Fingerabdruckes erfaßt wird. Transistoren zeichnen sich bekanntlich durch hohe Integrationsfähigkeit aus, ein derart gestalteter Sensor kann daher mit geringen Abmessungen, insbesondere geringer Dicke hergestellt werden.

Die Erfindung wird anhand von Figuren näher erläutert. Es zeigen beispielhaft:

Fig. 1 eine erfindungsgemäß gestaltete Chipkarte, Fig. 2 einen Querschnitt durch die Chipkarte nach Fig. 1,

Fig. 3 die Handhabung einer Chipkarte nach Fig. 1 und Fig. 2,

Fig. 4 eine schematische Darstellung des Ablaufes bei der Identifikationsprüfung und

Fig. 5 Aufbau eines Identifikationssystems, bei dem als biometrisches Identifikationsmerkmal die Netzhaut abgetastet wird.

Kernstück des erfindungsgemäßen Identifikationssystems ist die Chipkarte nach den Fig. 1, 2 und 3. Sie beinhaltet neben einer Speicher- und Vergleichslogik VSL, zwei aus einzelnen Transistoren aufgebaute Sensormatrizen SM, mit denen die Fingerabdrücke von Daumen D und Zeigefingers Z erfaßt werden. Um die Handhabung der Karte zu erleichtern, kann auch auf eine Sensormatrix und die Erfassung des Zeigefingerabdruckes verzichtet werden.

Die Stromversorgung der Chipkarte erfolgt über ein Schreib/Lesegerät SLG zu dem auch eine Datenverbindung besteht, über welche der für den vorgesehenen Anwendungszweck notwendige Datenaustausch erfolgt. Bei Einsatz der Chipkarte als elektronische Geldbörse handelt es sich dabei um Auf- bzw. Abbuchung von elektronischen Geldwerten.

Für den Identifikationsvorgang relevante Daten, wie beispielsweise das gespeicherte Fingerabdruckmuster werden über diese Datenverbindung nicht ausgetauscht, so daß diese Daten auch nicht über entsprechend präparierte Schreib/Lesegeräte ausgespäht werden können.

Die Sensormatrizen SM umfassen ein Raster von Transistoren, die so beschaltet sind, daß sie als Temperaturfühler dienen. Damit werden Hautrillenkuppen

und Hautrillensenken bei Anlegen eines Fingers auf die Sensormatrix über die Temperaturunterschiede erfaßt.

Anhand der Fig. 4 wird der Ablauf eines Identifikationsvorganges erläutert:

Bei dem Ausführungsbeispiel wird der Fingerabdruck in eine bestimmte Zahl von signifikanten Teilabdrücken zerlegt. Jeder Identifikationsvorgang bedient sich lediglich eines Teils der Teilabdrücke die zufällig oder pseudozufällig ausgewählt werden. Diese Auswahl AW ermöglicht eine, dem jeweiligen Sicherheitserfordernis angepaßte Vergleichsprozedur VP, die schnell bei geringen Ansprüchen und einer geringen Anzahl von Teilabdrücken abläuft, und entsprechend langsamer bei Hochsicherheitsanwendungen geschieht.

Die Auswahl der verwendeten Teilabdrücke kann ohne Einschränkung der Sicherheit auch durch das Schreib/Lesegerät SLG erfolgen.

Die ausgewählten Teilabdrücke werden vom biometrischen Erfassungssystem BM erfaßt und mit den gespeicherten und kryptologisch geschützten Daten SPD verglichen. Ergibt der Vergleich VP eine Übereinstimmung, dann wird die eigentliche Chipkartenfunktion CF, beispielsweise eine elektronische Geldbörse oder ein Zutrittschlüssel freigegeben.

Bei Nichtübereinstimmung erfolgen maximal zwei weitere Vergleichsvorgänge VV, wenn auch diese keine Übereinstimmung ergeben, wird die Chipkarte gesperrt SPE, wobei die Sperre zeitlich begrenzt sein kann.

Die Kartenpersonalisierung, d. h. die Speicherung bestimmter Fingerabdrücke auf einer Chipkarte geschieht wie folgt: Die "neue" Chipkarte wird vom Benutzer in das Schreib/Lesegerät eingebracht. Es ist dabei denkbar, daß nur ausgewählte Schreib/Lesegeräte beispielsweise in Banken zur Auslösung eines Personalisierungsvorganges berechtigt werden. Ein von dem Gerät ausgehender Initialisierungsimpuls veranlaßt dann die Speicher- und Vergleichslogik über die Sensormatrizen SM den/die Fingerabdrücke einzulesen und zu speichern. Danach ist keine Änderung dieser Daten mehr möglich.

Um in bestimmten Anwendungsfällen ein autorisiertes Auslesen und Verändern der Daten durch eine zentrale Stelle zu ermöglichen, kann eine kryptologisch geschützte Schnittstelle vorgesehen werden, wobei die auf der Chipkarte gespeicherten Daten entsprechend dem sogenannten RSA -Verfahren, wie es in der Zeitschrift Informationstechnik it 32 (1990), Seiten 24-32 "Algorithmen, Mechanismen und Dienste"; R. Oldenbourg Verlag beschrieben ist, mit dem "öffentlichen Teil" eines asymmetrischen Schlüsselverfahrens verschlüsselt werden.

Fig. 5 zeigt ein Identifikationssystem bei dem als biometrisches Identifikationsmerkmal die Netzhaut dient. Dabei hat der Benutzer durch ein Loch L in der Chipkarte eine Lichtquelle LQ im Schreib/Lesegerät zu blicken, so daß eine Visierlinie gebildet wird. Optische Sensoren S auf der dem Benutzer zugewandten Seite der Chipkarte erfassen dann die Struktur der Netzhaut.

Zur Erleichterung des Bedienungsvorganges umfaßt das Schreib/Lesegerät einen beweglichen Teil A, der die Chipkarte aufnimmt und an das Auge herangeführt werden kann. Der bewegliche Teil A ist mit dem Festteil B des Schreib/Lesegerätes mittels Kabel K verbunden.

Bevorzugte Anwendungsgebiete des erfindungsgemäßen Identifikationssystems sind insbesondere die elektronische Geldbörse, also der Ersatz von Bargeld und/oder Kreditkarten, Zugangs- und Zutrittskontrollen aller Art, damit insbesondere der Ersatz von mecha-

nischen Schlüsseln, die Personenidentifizierung und Authentifizierung, damit der Ausweisersatz, sowie der Einsatz als Datenspeicher z. B. für persönliche Daten wie die Ergebnisse von ärztlichen Untersuchungen.

Patentansprüche

1. Identifikationssystem mit elektronischer Chipkarte, mit Speichern für biometrische Identifikationsmerkmale der benutzungsberechtigten Personen, mit Sensoren zum Erfassen der biometrischen Identifikationsmerkmale und Mitteln zum Vergleich der gespeicherten und der erfaßten biometrischen Identifikationsmerkmale, **dadurch gekennzeichnet**, daß die Mittel zum Speichern (VSL), zur Erfassung (SM) und zum Vergleich (VSL) der biometrischen Identifikationsmerkmale jeweils zumindest teilweise in der Weise in die Chipkarte integriert sind, daß ein autonomer Vergleich der gespeicherten mit den erfaßten biometrischen Identifikationsmerkmale möglich ist und kein Austausch sicherheitsrelevanter Daten zwischen der elektronischen Chipkarte und den übrigen Komponenten des Identifikationssystems erfolgt.
2. Identifikationssystem nach Anspruch 1, dadurch gekennzeichnet, daß als biometrisches Identifikationsmerkmal zumindest ein Fingerabdruck einer benutzungsberechtigten Person vorgesehen ist.
3. Identifikationssystem nach Anspruch 2, dadurch gekennzeichnet, daß die Sensoren (SM) zum Erfassen des zumindest einen Fingerabdruckes ein Transistorarray beinhalten, und daß die Transistoren so geschaltet sind, daß das thermische Abbild des zumindest einen Fingerabdruckes erfaßt wird.
4. Identifikationssystem nach Anspruch 1, dadurch gekennzeichnet, daß als biometrisches Identifikationsmerkmal die Struktur der Netzhaut vorgesehen ist.

Hierzu 2 Seite(n) Zeichnungen

THIS PAGE BLANK (USPTO)

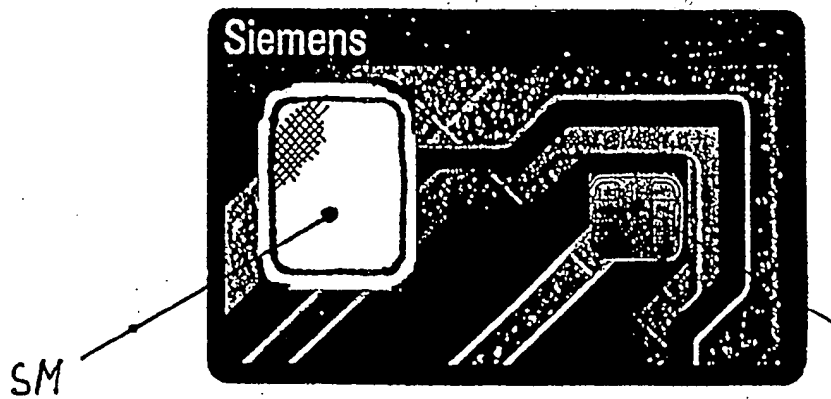


Fig. 1

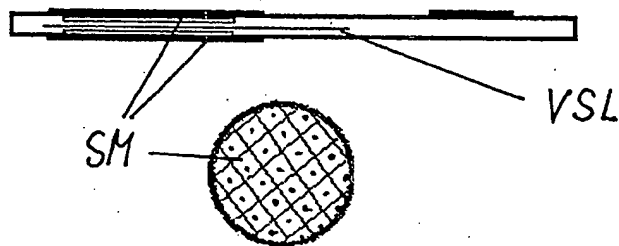


Fig. 2

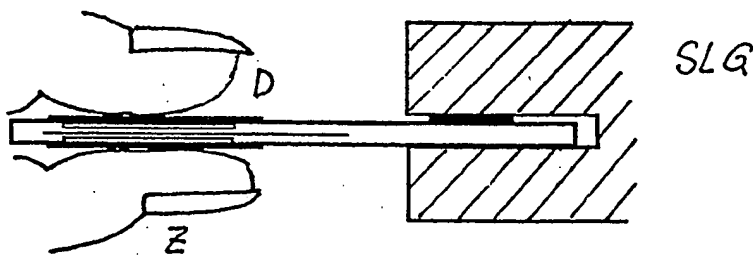


Fig. 3

BEST AVAILABLE COPY

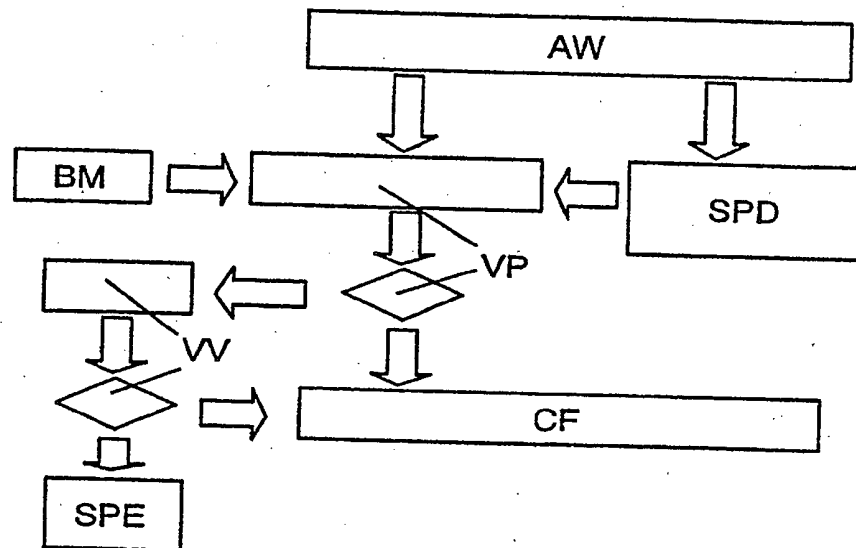


Fig.4

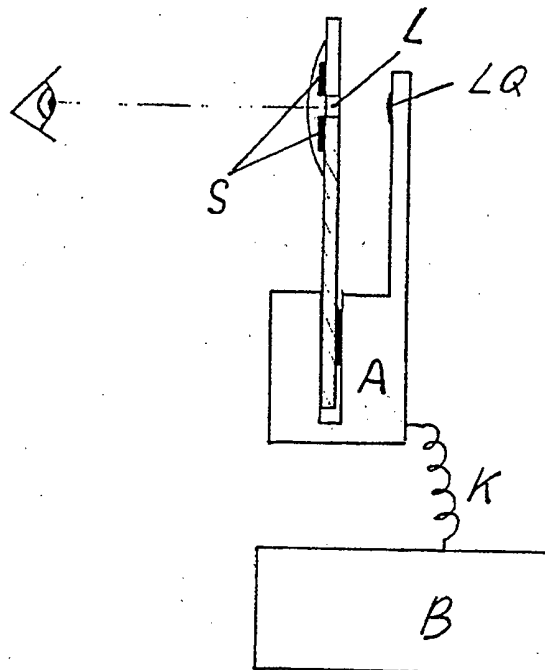


Fig.5